UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

TESLA, INC.,

Plaintiff,

v.

ALEX KHATILOV.

Defendant.

Case No.: ______________

DECLARATION OF DAVID SCHERTZER IN SUPPORT OF PLAINTIFF TESLA, INC.'S *EX PARTE* MOTION FOR TEMPORARY RESTRAINING ORDER, ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION, AND EVIDENCE PRESERVATION ORDER

Date: ______________
Time: ______________
Dept: ______________
Judge: ______________

Complaint To Be Filed

I, David Schertzer, affirm the following under penalty of perjury:

1. I work for Tesla, Inc. ("Tesla") as a Senior Security Intelligence Investigator. My duties include investigating data misuse on Tesla systems. I have personal knowledge of the facts set forth herein, and if called as a witness, could and would testify to them.

2. On the morning of January 6, 2021, Tesla's Information Security team, through monitoring software, identified employee Sabhir Khatilov (AKA Alex Tilov) as having moved thousands of files from Tesla networks to his personal Dropbox account, between December 31, 2020 and January 4, 2021. The software identified 26,377 filenames, though some duplicates appear to be present. Dropbox is a cloud-based file-storage program that is not part of the Tesla network.

3. The software used is our primary means for monitoring the Tesla network for misuse. We rely heavily on this software to identify when data is being exfiltrated. Throughout my investigations, this software has been reliable in identifying when people are improperly moving data off the network.

4. Immediately upon receiving this notification, the Information Security team reviewed the file transfer for validity and authorization. After determining that it was not a permitted transfer, the matter was escalated to me for investigation.

5. I promptly reviewed the transfer and determined that it included a great deal of highly confidential information, in violation of Tesla's data use policies. I showed the list of files that Mr. Khatilov transferred to Golda Arulappan, Mr. Khatilov's immediate supervisor and Senior Manager of Software Quality Assurance Engineering, who confirmed that these files included highly confidential Tesla Quality Assurance software scripts. Ms. Arulapan explained that these scripts automate a host of quality control tasks in Tesla's backend software, WARP Drive, and would be highly valuable in the hands of a competitor.

6. Later on January 6, 2021, I interviewed Mr. Khatilov via Microsoft Teams, a videoconferencing program. Ms. Arulappan participated in the interview, along with Investigator John Shumway and Jenna Ferrua, Acting Human Resources Director.

7. During the interview, Mr. Khatilov confirmed he had signed the Tesla Non-Disclosure Agreement, and that he understood the Agreement to mean he "should not share documents with anybody."

8. Mr. Khatilov confirmed that he used Dropbox and that he installed a Dropbox desktop application on his Tesla-issued laptop, which allowed him to rapidly upload files to his Dropbox account directly from his hard drive folder system.

9. When asked what files he uploaded to Dropbox, Mr. Khatilov claimed he only uploaded personal administrative documents, like his scanned passport and a copy of his W-4. When asked to clarify that Dropbox was used solely to upload administrative documents from the network, Mr. Khatilov again confirmed that.

10. In my experience, there are many easier way to get a few documents off the network—e.g. emailing documents to oneself. Installing a Dropbox client makes a massive exfiltration of thousands of documents possible without great effort.

11. I prompted Mr. Khatilov to screen share his laptop to confirm that his Dropbox account did not, as he twice claimed, contain any confidential Tesla files. Mr. Khatilov delayed

accepting the screen share request for over a minute, thus not allowing us to see the screen or to view his Dropbox files. During this time, I observed Mr. Khatilov on videochat rapidly clicking and typing. Because of these circumstances, I believe he was trying to modify Dropbox or other files to interfere with our inspection.

12. After Mr. Khatilov finally shared his screen, he claimed he had "already deleted" the Dropbox desktop application during the interview. Based on his behavior that I observed on videochat, I believe that Mr. Khatilov hurriedly deleted the application, and perhaps some files that were uploaded to Dropbox, while we were speaking and after we had already asked to inspect his account to see what he had stolen.

13. Although the desktop application had been removed from his Tesla laptop, my colleague Mr. Shumway instructed Mr. Khatilov to show all files that had already been transferred to Dropbox from the laptop. Deleting the Dropbox application disables the functionality that uploads files to a Dropbox account – it does not necessarily delete the files themselves. A review of those files revealed folders containing a very large amount of non-administrative material, including many of the Quality Assurance scripts that our monitoring software had detected as being transferred. We also instructed Mr. Khatilov to log into his Dropbox account on the Dropbox website, where the same Tesla files were still available through his account.

14. Mr. Khatilov agreed to delete the information from his laptop and the Dropbox account. Mr. Shumway instructed him how to permanently delete the files.

15. The remote nature of the interview necessarily hindered the process somewhat. Rather than in-person control over the actions of Mr. Khatilov, Mr. Shumway and I had to instruct him on particular actions to take, including folders to examine and files to click on. Due to the time constraints of the interview process, this was inherently restrictive.

16. After supervising the deletion, I then informed Mr. Khatilov that his Dropbox account contained non-administrative content and told him that Information Security had detected that he removed over 26,000 confidential filenames from the Tesla network. Khatilov claimed he didn't mention these before, despite being asked twice, because he "forgot."

17. Ms. Arulappan asked Mr. Khatilov what business purpose he had with these files. Mr. Khatilov was unable to articulate why he needed the files and did not provide any supporting details showing why he had downloaded them.

18. Throughout the interview Mr. Khatilov was terse and avoidant. He provided mostly one-word answers and feigned ignorance.

19. The whole interview lasted 49 minutes, roughly half of that time was spent attempting to delete the information.

20. Due to Mr. Khatilov's theft of trade secrets, as well as his repeated lying and obfuscation throughout the investigation, he was terminated that day.

21. Although we were able to delete information that we located on Mr. Khatilov's laptop and from his Dropbox account, we do not know whether he took additional files, whether the information was further transferred from Dropbox to other locations, or whether he shared the information with anyone else. From what we observed while instructing deletions during the interview, the files we deleted did not perfectly match the filenames our monitoring software identified as being uploaded. We were able to confirm some of the files were the same. However, I could not (and cannot) confirm that all the files uploaded to Dropbox were deleted. Moreover, from December 31 until January 6, when we supervised the deletion, any files could have been moved, copied, or accessed from Dropbox. We have no visibility into any transfers from Dropbox during this time, or from subsequent devices to other devices, if any.

22. As part of my job, I am aware of many of the protections Tesla uses to secure its confidential data. Tesla secures its physical facilities by restricting access to authorized personnel, and then monitoring actual access with security guards and cameras. Visitors to Tesla's facilities must check in with a receptionist or security guard, sign a nondisclosure agreement, and submit to a photograph. Visitors must further be escorted by a Tesla employee at all times.

23. Tesla also protects its confidential, proprietary, and trade secret information with stringent information security policies and practices. Tesla's network and servers are password-protected, firewall-protected, and accessible only to current Tesla employees with proper

credentials. Tesla also uses ongoing monitoring and investigation to identify attempts to exfiltrate confidential information from the Tesla network.

[*signature page follows*]

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Date: January 20, 2021

David Schertzer